PORTAL
USPTO

Subscribe (Full Service) Register (Limited Service, Free) Login

Search: ● The ACM Digital Library ○ The Guide

+signature +certificate +(integrity) +(storage repository docu SEARCH

THE ACM DIGITAL LIBRARY

Feedback Report a problem Satisfaction survey

Terms used:
signature certificate integrity storage repository document

Found **367** of **205,978**

Sort results by: relevance

Display results: expanded form

Save results to a Binder

Search Tips

□ Open results in a new window

Try an Advanced Search
Try this search in The ACM Guide

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next

Best 200 shown

Relevance scale

1 Trustworthy 100-year digital objects: Evidence after every witness is dead
Henry M. Gladney
July 2004 **ACM Transactions on Information Systems (TOIS)**, Volume 22 Issue 3
Publisher: ACM Press
Full text available: pdf(1.24 MB) Additional Information: full citation, abstract, references, citings, index terms

In ancient times, wax seals impressed with signet rings were affixed to documents as evidence of their authenticity. A digital counterpart is a message authentication code fixed firmly to each important document. If a digital object is sealed together with its own audit trail, each user can examine this evidence to decide whether to trust the content---no matter how distant this user is in time, space, and social affiliation from the document's source.We propose an architecture and design that a ...

2 Who's got the key?
David Henry
November 1999 **Proceedings of the 27th annual ACM SIGUCCS conference on User services: Mile high expectations SIGUCCS '99**
Publisher: ACM Press
Full text available: pdf(30.32 KB) Additional Information: full citation, references, index terms

Keywords: PKI, certificate authority, encryption

3 Antiquity: exploiting a secure log for wide-area distributed storage
Hakim Weatherspoon, Patrick Eaton, Byung-Gon Chun, John Kubiatowicz
March 2007 **ACM SIGOPS Operating Systems Review , Proceedings of the 2007 conference on EuroSys EuroSys '07**, Volume 41 Issue 3
Publisher: ACM Press
Full text available: pdf(584.64 KB) Additional Information: full citation, abstract, references, index terms

Antiquity is a wide-area distributed storage system designed to provide a simple storage service for applications like file systems and back-up. The design assumes that all servers eventually fail and attempts to maintain data despite those failures. Antiquity uses a secure log to maintain data integrity, replicates each log on multiple servers for durability, and uses dynamic Byzantine fault-tolerant quorum protocols to ensure consistency among replicas. We present Antiquity's design and an ...

Keywords: archival storage systems, data durability, data integrity, distributed storage system, wide-area

4 IS '97: model curriculum and guidelines for undergraduate degree programs in information systems
Gordon B. Davis, John T. Gorgone, J. Daniel Couger, David L. Feinstein, Herbert E. Longenecker
December 1996 **ACM SIGMIS Database , Guidelines for undergraduate degree programs on Model curriculum and guidelines for undergraduate degree programs in information systems IS '97**, Volume 28 Issue 1
Publisher: ACM Press
Full text available: pdf(7.24 MB) Additional Information: full citation, citings

5 Computing curricula 2001
September 2001 **Journal on Educational Resources in Computing (JERIC)**
Publisher: ACM Press
Full text available: pdf(613.63 KB) html(2.78 KB) Additional Information: full citation, references, citings, index terms

6 Authentication and signature schemes: Origin authentication in interdomain routing
William Aiello, John Ioannidis, Patrick McDaniel
October 2003 **Proceedings of the 10th ACM conference on Computer and communications security CCS '03**
Publisher: ACM Press
Full text available: pdf(268.26 KB) Additional Information: full citation, abstract, references, citings, index terms

Attacks against Internet routing are increasing in number and severity. Contributing greatly to these attacks is the absence of *origin authentication*: there is no way to validate claims of address ownership or location. The lack of such services enables not only attacks by malicious entities, but indirectly allow seemingly inconsequential miconfigurations to disrupt large portions of the Internet. This paper considers the semantics, design, and costs of origin authentication in interdomai ...

Keywords: BGP, address management, delegation, routing, security

7 Decentralized storage systems: Farsite: federated, available, and reliable storage for an incompletely trusted environment
Atul Adya, William J. Bolosky, Miguel Castro, Gerald Cermak, Ronnie Chaiken, John R. Douceur, Jon Howell, Jacob R. Lorch, Marvin Theimer, Roger P. Wattenhofer
December 2002 **ACM SIGOPS Operating Systems Review**, Volume 36 Issue SI
Publisher: ACM Press
Full text available: pdf(1.87 MB) Additional Information: full citation, abstract, references, cited by, index terms

Farsite is a secure, scalable file system that logically functions as a centralized file server but is physically distributed among a set of untrusted computers. Farsite provides file availability and reliability through randomized replicated storage; it ensures the secrecy of file contents with cryptographic techniques; it maintains the integrity of file and directory data with a Byzantine-fault-tolerant protocol; it is designed to be scalable by using a distributed hint mechanism and delegatio ...

8 Secure Data Publishing and Certificate Management: Flexible authentication of XML documents
P. Devanbu, M. Gertz, A. Kwong, C. Martel, G. Nuckolls, S. G. Stubblebine
November 2001 **Proceedings of the 8th ACM conference on Computer and Communications Security CCS '01**
Publisher: ACM Press
Full text available: pdf(219.17 KB) Additional Information: full citation, abstract, references, citings, index terms

XML is increasingly becoming the format of choice for information exchange, in critical areas such as government, finance, healthcare and law, where integrity is of the essence. As this trend grows, one can expect that documents (or collections thereof) may get quite large, and clients may wish to query for specific segments of these documents. In critical applications, clients must be assured that they are getting complete and correct answers to their queries. Existing methods for signing XML d ...

9 Fast detection of communication patterns in distributed executions
Thomas Kunz, Michiel F. H. Seuren
November 1997 **Proceedings of the 1997 conference of the Centre for Advanced Studies on Collaborative research CASCON '97**
Publisher: IBM Press
Full text available: pdf(4.21 MB) Additional Information: full citation, abstract, references, index terms

Understanding distributed applications is a tedious and difficult task. Visualizations based on process-time diagrams are often used to obtain a better understanding of the execution of the application. The visualization tool we use is Poet, an event tracer developed at the University of Waterloo. However, these diagrams are often very complex and do not provide the user with the desired overview of the application. In our experience, such tools display repeated occurrences of non-trivial commun ...

10 Control and integrity: New techniques for ensuring the long term integrity of digital archives
Sangchul Song, Joseph JaJa
May 2007 **Proceedings of the 8th annual international conference on Digital government research: bridging disciplines & domains dg.o '07**
Publisher: Digital Government Research Center
Full text available: pdf(607.08 KB) Additional Information: full citation, abstract, references, index terms

A large portion of the government, business, cultural, and scientific digital data being created today needs to be archived and preserved for future use of periods ranging from a few years to decades and sometimes centuries. A fundamental requirement of a long term archive is to ensure the integrity of its holdings. In this paper, we develop a new methodology to address the integrity of long term archives using rigorous cryptographic techniques. Our approach involves the generation of a small ...

Keywords: data integrity, digital archives, integrity audits, linked hashing

11 COCA: A secure distributed online certification authority
Lidong Zhou, Fred B. Schneider, Robbert Van Renesse
November 2002 **ACM Transactions on Computer Systems (TOCS)**, Volume 20 Issue 4
Publisher: ACM Press
Full text available: pdf(448.28 KB) Additional Information: full citation, abstract, references, citings, index

terms

COCA is a fault-tolerant and secure online certification authority that has been built and deployed both in a local area network and in the Internet. Extremely weak assumptions characterize environments in which COCA's protocols execute correctly: no assumption is made about execution speed and message delivery delays; channels are expected to exhibit only intermittent reliability; and with $3t + 1$ COCA servers up to t may be faulty or compromised. COCA is the first system to integr ...

Keywords: Byzantine quorum systems, Certification authority, denial of service, proactive secret-sharing, public key infrastructure, threshold cryptography

12 Certificate-based authorization policy in a PKI environment
Mary R. Thompson, Abdelilah Essiari, Srilekha Mudumbai
November 2003 **ACM Transactions on Information and System Security (TISSEC)**, Volume 6 Issue 4
Publisher: ACM Press
Full text available: pdf(233.63 KB) Additional Information: full citation, abstract, references, citings, index terms

The major emphasis of public key infrastructure has been to provide a cryptographically secure means of authenticating identities. However, procedures for authorizing the holders of these identities to perform specific actions still need additional research and development. While there are a number of proposed standards for authorization structures and protocols such as KeyNote, SPKI, and SAML based on X.509 or other key-based identities, none have been widely adopted. As part of an effort to us ...

Keywords: Public key infrastructure, XML, digital certificates

13 Bidirectional mobile code trust management using tamper resistant hardware
John Zachary, Richard Brooks
April 2003 **Mobile Networks and Applications**, Volume 8 Issue 2
Publisher: Kluwer Academic Publishers
Full text available: pdf(152.99 KB) Additional Information: full citation, abstract, references, index terms

Trust management in a networked environment consists of authentication and integrity checking. In a mobile computing environment, both remote hosts and mobile code are suspect. We present a model that addresses trust negotiation between the remote host and the mobile code simultaneously. Our model uses tamper resistant hardware, public key cryptography, and one-way hash functions.

Keywords: authentication, hash functions, mobile code, tamper resistant hardware, trust management

14 Digital signatures: can they be accepted as legal signatures in EDI?
Patrick W. Brown
December 1993 **Proceedings of the 1st ACM conference on Computer and communications security CCS '93**
Publisher: ACM Press
Full text available: pdf(809.34 KB) Additional Information: full citation, abstract, references, citings, index terms

Digital Signature (DS) technology may be employed to produce legally enforceable signatures in Electronic Data Interchange (EDI) among computer users within the same general guidelines and requirements as those developed for handwritten signatures on paper. Digital signature technology promises assurance at least equal to written signatures. From a legal standpoint, this assurance remains to be tested in the evidentiary process. Business policies for organizational use of this technology ar ...

Keywords: EDI, cryptography, digital signatures, distributed systems, law

15 Semantic Web foundations: Named graphs, provenance and trust
Jeremy J. Carroll, Christian Bizer, Pat Hayes, Patrick Stickler
May 2005 **Proceedings of the 14th international conference on World Wide Web WWW '05**
Publisher: ACM Press
Full text available: pdf(130.32 KB) Additional Information: full citation, abstract, references, citings, index terms

The Semantic Web consists of many RDF graphs nameable by URIs. This paper extends the syntax and semantics of RDF to cover such Named Graphs. This enables RDF statements that describe graphs, which is beneficial in many Semantic Web application areas. As a case study, we explore the application area of Semantic Web publishing: Named Graphs allow publishers to communicate assertional intent, and to sign their graphs; information consumers can evaluate specific graphs using task-specific trust pol ...

Keywords: RDF, provenance, semantic Web, trust

16 Exchange of patient records-prototype implementation of a security attributes service in X.500
Marjan Jurečič, Herbert Bunz
November 1994 **Proceedings of the 2nd ACM Conference on Computer and communications security CCS '94**
Publisher: ACM Press
Full text available: pdf(884.04 KB) Additional Information: full citation, abstract, references, index terms

In Europe, the use of computers in health care industry has increased rapidly in recent years. This increase, however, has been accomplished with research efforts in the area of privacy and confidentiality of personal data. In the German legislation, protection of personal data is guaranteed by the constitution, granting a general right to privacy. This constitutional right has been amended by the German Central Court (Bundesverfassungsgericht). It says that each individual has the right to ...

17 A wide-area Distribution Network for free software
Arno Bakker, Maarten Van Steen, Andrew S. Tanenbaum
August 2006 **ACM Transactions on Internet Technology (TOIT)**, Volume 6 Issue 3
Publisher: ACM Press
Full text available: pdf(215.08 KB) Additional Information: full citation, abstract, references, index terms

The Globe Distribution Network (GDN) is an application for the efficient, worldwide distribution of freely redistributable software packages. Distribution is made efficient by encapsulating the software into special distributed objects which efficiently replicate themselves near to the downloading clients. The Globe Distribution Network takes a novel, optimistic approach to stop the illegal distribution of copyrighted and illicit material via the network. Instead of having moderators check the p ...

Keywords: Distributed objects, copyright, file sharing, middleware, software distribution, traceable content, wide-area networks

18 OceanStore: an architecture for global-scale persistent storage

John Kubiatowicz, David Bindel, Yan Chen, Steven Czerwinski, Patrick Eaton, Dennis Geels, Ramakrishna Gummadi, Sean Rhea, Hakim Weatherspoon, Chris Wells, Ben Zhao

November 2000 **ACM SIGARCH Computer Architecture News , ACM SIGOPS Operating Systems Review , Proceedings of the ninth international conference on Architectural support for programming languages and operating systems ASPLOS-IX**, Volume 28 , 34 Issue 5 , 5

Publisher: ACM Press

Full text available: pdf(166.53 KB) Additional Information: full citation, abstract, references, citings, index terms

OceanStore is a utility infrastructure designed to span the globe and provide continuous access to persistent information. Since this infrastructure is comprised of untrusted servers, data is protected through redundancy and cryptographic techniques. To improve performance, data is allowed to be cached anywhere, anytime. Additionally, monitoring of usage patterns allows adaptation to regional outages and denial of service attacks; monitoring also enhances performance through pro-active movement ...

19 OceanStore: an architecture for global-scale persistent storage

John Kubiatowicz, David Bindel, Yan Chen, Steven Czerwinski, Patrick Eaton, Dennis Geels, Ramakrishan Gummadi, Sean Rhea, Hakim Weatherspoon, Westley Weimer, Chris Wells, Ben Zhao

November 2000 **ACM SIGPLAN Notices**, Volume 35 Issue 11

Publisher: ACM Press

Full text available: pdf(1.47 MB) Additional Information: full citation, abstract, references, citings, index terms

OceanStore is a utility infrastructure designed to span the globe and provide continuous access to persistent information. Since this infrastructure is comprised of untrusted servers, data is protected through redundancy and cryptographic techniques. To improve performance, data is allowed to be cached anywhere, anytime. Additionally, monitoring of usage patterns allows adaptation to regional outages and denial of service attacks; monitoring also enhances performance through pro-active movement ...

20 Authentication: Message authentication by integrity with public corroboration

P. C. van Oorschot

September 2005 **Proceedings of the 2005 workshop on New security paradigms NSPW '05**

Publisher: ACM Press

Full text available: pdf(2.31 MB) Additional Information: full citation, abstract, references, index terms

One of the best-known security paradigms is to use authentication as the basis for access control decisions. We turn this around, and instead rely on access control (or more precisely, integrity) as the basis for authentication. We propose a simple, practical means by which data origin assurances for message authentication are based on corroboration, for example by cross-checking with information made available by a known source or at a specified location (e.g., web page). The security re ...

Keywords: data origin authentication, digital signatures, email source authentication, message authentication, phishing, security by integrity, spam, undetected key compromise

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	2462	(713/176).CCLS.	US-PGPUB; USPAT	OR	OFF	2007/07/06 17:12
S2	1247	(713/176).CCLS.	US-PGPUB	OR	OFF	2007/07/03 21:24
S3	384	((713/179) or (713/181)).CCLS.	USPAT	OR	OFF	2007/07/03 21:24
S4	1215	(713/176).CCLS.	USPAT	OR	OFF	2007/07/03 21:24
S5	420	((stor$3 sav$3) with certificate with (mac hash check adj code digest))	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/03 21:28
S6	2462	(713/176).CCLS.	US-PGPUB; USPAT	OR	OFF	2007/07/03 21:28
S7	52	((stor$3 sav$3) with certificate with (mac hash check adj code digest)) and (S6 S3)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/03 21:34
S8	1	("6795834").PN.	US-PGPUB; USPAT	OR	OFF	2007/07/03 21:30
S9	21	((stor$3 sav$3) with certificate with signature with (mac hash check adj code digest)) and (S6 S3)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/06 17:27
S10	11	((stor$3 sav$3) with certificate with signature with (mac hash check adj code digest)).clm.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/03 21:41
S11	0	(certificate with signature with check adj code).clm.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/03 21:41
S12	2	(certificate with signature with check adj code)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/03 22:02

EAST Search History

S13	1	("20040162982").PN.	US-PGPUB; USPAT	OR	OFF	2007/07/03 22:02
S14	1	nakahara-shinichi.in. and (data adj storage and recording adj medium). ti.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/05 18:29
S15	1	nakahara.in. and (data adj storage and recording adj medium).ti.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/05 18:29
S16	2	nakahara.in. and (data adj storage). ti.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/05 18:31
S17	2	kanai.in. and (electronic adj document adj management adj system).ti.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/05 18:33
S18	47	shinichi.in. and (data adj storage).ti.	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/05 18:31
S19	18	kanai.in. and (signature with hash)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/05 21:28
S20	17	entry adj signature with hash	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/05 21:33
S21	39	kanai.in. and (signature)	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/05 21:35

S22	301	storage adj signature	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/05 21:50
S23	1	nakahara.in. and storage adj signature	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/05 21:36
S24	0	"hash of the signature" "hash of the digital signature"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/05 21:50
S25	351	hash adj signature	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/05 21:50
S26	248	("5005200").URPN.	USPAT	OR	ON	2007/07/05 21:53
S27	2	"6950943"	US-PGPUB; USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/06 17:12
S28	9	("5414844" | "5483596" | "5787428" | "6105131" | "6178422" | "6253193" | "6292904" | "6314409" | "6839843").PN.	US-PGPUB; USPAT; USOCR	OR	ON	2007/07/06 17:25
S29	0	(stor$3) with (certificate) with siganture	US-PGPUB; USPAT; USOCR	OR	ON	2007/07/06 17:26
S30	1512	(stor$3) with (certificate) with signature	US-PGPUB; USPAT; USOCR	OR	ON	2007/07/06 17:26
S31	384	((713/179) or (713/181)).CCLS.	USPAT	OR	OFF	2007/07/06 17:27
S32	2464	(713/176).CCLS.	US-PGPUB; USPAT	OR	OFF	2007/07/06 17:27

EAST Search History

S33	173	((stor$3 sav$3) with certificate with signature) and (S32 S31)	US-PGPUB;
			USPAT;
			USOCR;
			EPO; JPO;
			DERWENT;
			IBM_TDB
				OR	ON	2007/07/06 17:27